UIFAND
FINANCIAL INTELLIGENCE UNIT
PRINCIPALITY OF ANDORRA

INFORMATIVE NOTE ADDRESSED TO THE NON-BANKING FINANCIAL SECTOR REGARDING THE ONGOING MONITORING OF BUSINESS RELATIONSHIPS, RECORD KEEPING AND UPDATING

Date: 23 January 2020

Purpose: To provide reporting entities with aggregate conclusions and recommendations in order to improve their internal control procedures with respect to the ongoing monitoring of business relationships, the scrutiny of transactions, the updating of documents obtained within the framework of the application of due diligence measures, and the keeping of such documents.

Rationale

The systems for the prevention of money laundering and terrorist financing should comprise customer onboarding controls and the monitoring of continued relations. Notwithstanding, the thoroughness of the verifications made by reporting entities is usually deeper at the start of business relations than in subsequent checks.

For this reason, UIFAND has performed a thematic inspection in the course of 2019 for the purpose of evaluating the level of compliance of reporting entities with the legal requirements relating to the adequacy and validity of the documents, information and data obtained within the framework of the application of due diligence measures, and the keeping and digitalization of same. Additionally, the scope of the inspection included the systems for the continuous monitoring of business relationships and for the scrutiny of transactions.

This inspection covered several entities within the group of non-banking financial entities, including investment companies, asset management companies and financial advisers, considering the large percentage of long-term business relations that they involve and the significant number of transactions connected with such business relations, primarily with respect to the provisions and reimbursements of the managed and/or advised assets.

This document sets out the main conclusions, risk areas and recommended actions detected within the framework of said inspections, making them available to all reporting entities as a whole and particularly to the rest of the financial reporting entities, that is to say, to the insurance and banking sector in view of its likewise significant volume of long-term business relationships and the transactions involved, as well as to the general public.

General conclusions on the thematic inspection regarding the ongoing monitoring of business relationships, record keeping and updating.

Generally speaking, the controls implemented by the inspected reporting entities are satisfactory as regards the updating and keeping of documents within the framework of the monitoring of business relations. In particular, with respect to record keeping, it was found that reporting entities correctly keep, in both physical and digital format, all the documents related to the verified business relationships from the start of such relationships. Moreover, they usually keep earlier versions of the documents that they obtain and of the checks that they perform, keeping the most recent and updated versions as well.

In general, the reporting entities' control systems in this area are mainly managed manually, although the larger entities have computer applications that allow the scrutiny of transactions to be carried out in greater detail. In any case, however, the implemented control systems are usually consistent with the complexity and size of the business, so they are applicable and appropriate in practice. Despite this, it is also commonly found that the control procedures which are carried out in practice are not formalized in internal manuals, which sometimes contrast considerably with the reality of the respective business.

Even so, it should be underscored that major efforts and substantial investments have been made in the automation of control systems and in developments aimed to ensure the availability and validity of the customers' documents and information.

Detected risk areas and recommended improvement actions

Despite the general conclusions presented in the previous section, UIFAND's various supervisory actions have led to the detection of a series of risk areas. Here we present a set of recommended actions conceived to improve the effectiveness of the reporting entities' prevention systems.

The recommendations are not only related to the monitoring and updating of documents of business relationships but also to the procurement of the documents which have to subsequently be kept and updated.

1. *General considerations on the ongoing monitoring of business relationships and on record keeping and updating*

   1.1. *Updating of outdated documents*

Detected risks
• The periodicities for the update of supporting documents are not always fully in line with the customer's risk, the type of document, the purpose and nature of the business relationship, or even with the internal procedures defined to ensure the validity of the documents. • Sometimes it is not taken into account that documents may lose their validity not only because their expiration date elapses, but also because the situation intended to justify is no longer the current situation.
Recommended improvement actions
• Clearly identify the type of supporting documents obtained within the framework of the application of due diligence measures that are subject to periodic updating, and establish the update frequency by means of internal rules. Ensure in all cases that the updating of the respective documents complies with the defined periods. • Adjust the volume of documents and update them in accordance with customers' risk levels instead of taking the type of documents concerned as the sole basis for these actions. • Consider the implementation of IT tools that will allow automated alerts to be established in order to detect forthcoming expirations of customer documents.

   1.2. *Systems for continuous monitoring of business relations and the scrutiny of transactions*

Detected risks
• On the whole, the entities possess systems that allow them to carry out a continuous monitoring of their business relations and scrutinize the transactions they provide, with a higher or lower level of automation depending on their businesses' size and complexity.

Nevertheless, these systems may be subject to being reviewed in order to increase their scope and checking criteria, their updating, the frequency of the checks and the documentation of the analyses carried out.
Recommended improvement actions
• Clearly define the scope of the transactions subject to verification within the framework of the continuous monitoring of business relationships (deposits, reimbursements, transfers of funds between accounts of the same customer within the entity, etc.) and the verification criteria (it is recommendable to take into account various risk factors and not only specific amount thresholds). • Strengthen the transaction scrutiny controls in the services which entail a greater risk, such as in the case of direct asset management, in which funds are deposited or reimbursed into omnibus accounts of the entity. • The analyses conducted as a result of the internal procedures for the control of transactions should be documented in written form and it should be ensured that such analyses have been carried out on the basis of supporting documents (deeds of acceptance of inheritance, donations in front of a public notary, etc.), preferably originating from reliable and independent sources.

1.3. *Keeping of documents obtained within the framework of the application of due diligence measures and of the analyses carried out*

Detected risks
• The reporting entities have implemented procedures to ensure the keeping of and access to the information obtained from the application of due diligence measures, usually from the start of the business relationship, which may even exceed the minimum period of time provided by Article 37.1 of *Law 14/2017.* Despite this, however, certain types of actions are not usually included within the scope of the documents to be kept.
Recommended improvement actions
• Ensure that all types of analyses carried out in the course of the business relation (within the framework of the continuous monitoring of the business relation, and of the scrutiny of transactions, at the time of determining the beneficial owner, the consistency analyses performed on the source of the funds/assets, the reclassifications of customer risk, etc.) are documented in writing and are subject to the same updating, keeping and accessing procedures which are applied to other types of documents, such as identification documents.

2. *Classification of customers' risk and its relation with the amount of documentation and updating frequency.*

2.1. *Classification of customer risk and reassessment*

Detected risks
• Although in the great majority of cases the systems for classification of customers according to their ML/TF risk level are implemented and formalized, they tend to be subject to improvements in terms of the risk criteria to be taken into account for the calculation. • It is also necessary to establish periodic reassessments of both the system and customers in order to detect situations which are susceptible to increase or decrease customer risk, making this procedure a dynamic tool that considers the various events and operations of the business relationship instead of a static tool that is only taken into consideration at the start of the business relationship.

- Sometimes the entities organize their business relations internally at the level of portfolios, accounts or contracts but not at a customer level, which makes it hard to achieve an overall view of customers and may have an influence on customers' correct classification in terms of ML/TF risk, and on the application of due diligence measures.

Recommended improvement actions

- Firstly, and in the event in which this is not the case, the customer risk classification system should be formalized in writing, specifying the risk factors to be considered and the calculation method.
- Ensure that the customer risk classification systems take into account all the significant risk factors, such as familiar, business or ties of any other nature that the customer might have and may be important in determining their risk profile, even if the associated persons or entities are not customers of the entity.
- From a legislation standpoint, there are risk scenarios in which it is required to adopt enhanced due diligence measures that prevail over the measures which would otherwise be applicable on the basis of the entity's internal risk classification. These scenarios are provided in Articles 12 to 17 of *Law 14/2017* as well as in specific UIFAND Technical Communiqués which are in force, such as those relating to risk countries or the Technical Communiqué CT-04/2014.
- It is recommendable to date risk assessments and to establish a procedure for verifying their validity, with a defined periodicity and based on the resulting risk. Moreover, a documentary record should be kept of any change of the previously assigned risk level.
- In the event in which the entity has an IT system for the management of customers' documents and/or information, it is recommendable that the customer risk classification system should obtain the information directly from the system to perform the pertinent calculations.
- Define the parameterization of the tool for performing the risk calculation so that manual changes are avoided as much as possible. In exceptional cases in which manual changes cannot be avoided, ensure that the assigned risk is recorded consistently on all the customer documents which are kept, avoiding mentions of different risk levels in the same file, and ensuring that due diligence measures are applied consistently to the real AML/CFT risk that has been determined.
- An ML/TF risk classification should be assigned to the customer and not to the portfolio in the cases in which the same customer appears in more than one portfolio, in order to adjust the amount of documents to obtain and the updating and control processes to be applied by the entity on the basis of customers' risk level.

2.2. *Gradation of due diligence measures according to customers' risk classification: volume and updating*

Detected risks

- Sometimes notable variations are not observed in either the volume of documents obtained or the intensity of the controls which are applied according to customers' risk classification. This causes situations in which the business relationships of higher risk do not show a substantially enhanced control in comparison to the business relationships identified as being of medium or low risk. Similarly, the reclassification of business relationships to a higher risk level, with an increase in their periodicity of verification, does not influence the scope of the due diligence measures which are applied, as the reporting entity considers that it has already obtained all the possible documents.

Such situation would be explained by the fact that the documents which are possessed on the customers would not only include the documents which are required by the internal procedures, but also the documents to which the reporting entity has had access for various reasons in the course of the business relation and therefore there is not always a correlation between the customer's risk classification, the due diligence measures which are adopted, and the information and documents which are obtained. Consequently, reporting entities face difficulties in establishing uniform procedures for the updating of documents and the monitoring of business relationships.
Recommended improvement actions
• Review the criteria established to grade the application of due diligence measures on the basis of the risk levels resulting from the classification of customers, adjusting the volume of documents obtained and the updating and control processes according to customers' risk levels.

3. *Procurement of documents relating to the application of due diligence measures and the updating of such documents*

3.1. *Identification of the beneficial owner and updating of the analysis*

Detected risks
• The fact that customers are and/or represent complex structures makes the task of identifying their beneficial owner or owners more difficult. The risk for this increases if the beneficial owner is only identified at the start of the business relationship and a periodic reassessment of the status is not carried out.
Recommended improvement actions
• In the case of customers which are legal entities and especially if they involve complex structures, ensure the procurement of all the necessary documents to determine the identity of the beneficial owner through an analysis of all the intermediary companies. This analysis should be carried out on documents obtained from reliable independent sources and the documents should be sufficient to suitable to identify and verify the identity. Accordingly, in such cases it would not suffice to possess only a sworn statement signed by the customer. • All possible efforts should be made to obtain access, either directly or indirectly, to reliable independent sources, such as national or foreign public registers, that are sufficient to ensure that the identification and verification of the identity of the beneficial owner are carried out in compliance with the legislation in force in matters of AML/TF. • A periodic reassessment should be made of the analysis carried out to determine the identity of the beneficial owners of customers in order to ensure that the identity of the beneficial owners is known at all times, thus allowing the detection of any change in the control and/or ownership of the funds deposited in the account or, at least, whenever transactions are carried out. This reassessment should be performed in accordance with the assigned risk level whenever the customer's operations show signs of a possible change of beneficial owner or when any significant event has occurred that justifies such reassessment. In any case, the periodicity of review may not be higher than the one established in the UIFAND Technical Communiqué CT-02/2019 (5 years).

3.2. *Documents and analyses relating to the knowledge about the customer and their updating*

Detected risks

- A suitable knowledge about the customer is indispensable in order to assign an appropriate risk classification and to be able to detect potential suspicious activities. Moreover, the information and knowledge possessed in connection with the customer should not be static, but rather it should vary over the course of the business relationship depending, among other things, on the operations which the customer carries out.

  A lack of analysis and of knowledge of the customer, and an inadequate formalization and updating of the documents obtained, are vulnerabilities of control systems.

- An incorrect identification of the customer's sector of activity could entail an inadequate application of due diligence measures. This would be the case, for example, if foundations constituted in offshore jurisdictions which are devoted to the management of particular assets, were to be classified as NPOs.

Recommended improvement actions

- Documentary records should be made of the analyses carried out in searches of open sources or of the documents provided by customers, especially in the cases in which there are records of negative news reports and/or information inconsistent with the knowledge possessed of the customer. Likewise, a documentary record should be made of the decision that is adopted in the assessment of a potential suspicion.

- In the business relationships of high risk, the knowledge about the customer should be enhanced in comparison to low-risk business relationships, for example with specific AML/CFT reports or memorandums.

- In the case of NPO customers, it is indispensable to possess the knowledge that the respective organization (association, foundation or other) is engaged in raising or disbursing funds for charitable, religious, cultural, educational, social, fraternal purposes, or for the carrying out of other types of "good works". Such knowledge should allow the correct identification and risk categorization of the customer, and the adjustment of the continuous monitoring controls of the business relationship in order to detect risk scenarios specific to the sector.

- The documents relating to the knowledge of the customer should be updated with a periodicity defined on the basis of the customer's risk.

3.3. *Source of funds and updating of the analysis*

Detected risks

- In some business relationships the managed or advised assets were generated by the customer many years earlier, a circumstance that makes it hard to identify and to obtain sufficient information to prove the source of the funds.

- In other cases, the business relationships are of long standing and date back several decades. For this reason they may have not been put to an analysis of the source of funds or they may have been indeed analysed in this respect but with a different criteria from that established by the reporting entities at the present time. Similarly, in the cases in which the analyses were performed, they may also have been subject to a deficient updating.

- Likewise, on some occasions the justification of the customer's professional activity is mixed up with the justification of the source of funds, considering that the justification of one of these aspects (usually the professional activity) is sufficient proof for both aspects, without assessing whether such professional activity has been the origin of the managed

or advised assets. A lack of assessment of the sufficiency of the documents relating to the origin of funds, and a periodic reassessment of such sufficiency (whether this should be done according to periods of time defined by internal rules or every time that a significant event, such as the provision of new funds, occurs) may entail a risk with respect to the correct detection of suspicious activity.
Recommended improvement actions
• Documentary records should be made of the analysis carried out on the origin of funds and of the conclusion reached with respect to the sufficiency of the documents obtained. • Enhanced proof of the source of funds should be obtained especially for high-risk business relationships in the case in which, despite having compiled documents relating to the customer's professional activity and to the income that it generates, the documents are not sufficient to justify the total volume of the managed assets. • In the cases in which the assets that are the object of the business relationship were generated long ago and, therefore, the origin of such assets is difficult to prove by today's internal procedures, the greatest possible effort should be made to prove the origin of such funds with the all the possible information and/or documents, even if they are not the precise same standard information or documents that the entity requires. In cases such as these in which information and/or documents of a different type are obtained and in which they consequently call for an analysis of their sufficiency, it is additionally recommended that a record should be made in the customer's file on the analysis which is carried out and it should be assessed whether this circumstance should or should not have implications for the customer's ML/TF risk classification.

4. *Other matters*

4.1. *Operations alien to the service provided*

Detected risks
• Sometimes the management or advisory service is performed on accounts in which the customer carries out operations of his own, which makes it more difficult to carry out the pertinent control tasks for the scrutiny of transactions.
Recommended improvement actions
• In the cases in which the management or advisory service is provided on assets deposited in a bank account held in the name of the customer, it is highly recommendable that the operations which are made through such account should be limited to the investment or divestment transactions which are advised or managed by the entity, without there being any operations involving other activities of the customer. Otherwise, the scrutiny of transactions should cover, in addition, the movements made by the customer himself in such account, regardless of whether or not they bear any relation to the purpose of the business relationship.

4.2. *Identification of designated persons and entities, and application of restrictive measures and updating of the procedure.*

Detected risks
• The use of private sources (for example, *Namebook*, *World-Check*, *Dow Jones*, or others) is commonly found to be widespread in the sector. Despite this, these applications are used to carry out multiple verifications at one time in relation to the whole customer portfolio, for which the measures to be applied, according to the legislation, differ, such as detecting

the PEP status of a customer or detecting persons and entities designated by international organisations. This circumstance may entail that the scope and periodicity defined for searches in the private sources applications will not be sufficient to ensure compliance with all the obligations defined in *Law 14/2017*, especially with respect to the application of restrictive measures on persons and entities designated by the United Nations Security Council for their ties with terrorism and its financing or with the financing of the proliferation of weapons of mass destruction, according to the definition of Chapter 9 of the aforementioned Law.
Recommended improvement actions
• The search process in external private sources applications should be formalized in the internal manual, establishing the criteria with respect to the match percentage, the included lists, the scope of verification (customer's full name), etc., and ensuring that such criteria remain the same over the course of time in order to allow the detection of new additions to the lists. Moreover, the procedure should ensure that the version of the lists which are used is the most recently updated version. • A record should be made of the verification carried out with respect to matches, including cases of evident false positives. • It should be ensured that the periodicity established in the verification procedure with the Consolidated List of the United Nations Security Council, whether or not it is carried out through external applications of private sources, provides assurance of the detection of persons and entities who have ties with terrorist activities or the financing of same, or the financing of the proliferation of weapons of mass destruction, and that the application of restrictive measures within the terms set by *Law 14/2017* is ensured. • It should be recalled that the service providers of private sources allow the performance of joint searches of the whole portfolio of customers and beneficial owners, among other aspects.

Supervision Area